(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 11039262 A

(43) Date of publication of application: 12 . 02 . 99

(51) Int. Cl G06F 15/00
G06F 9/06
G06F 12/14
G09C 1/00
G11B 20/10
H04L 9/32

(21) Application number: 09196212

(22) Date of filing: 22 . 07 . 97

(71) Applicant: FUJITSU LTD

(72) Inventor: MATSUMOTO TATSURO
ISOMICHI HIROYO
HIRAGA MASAHIRO
ITO CHIAKI

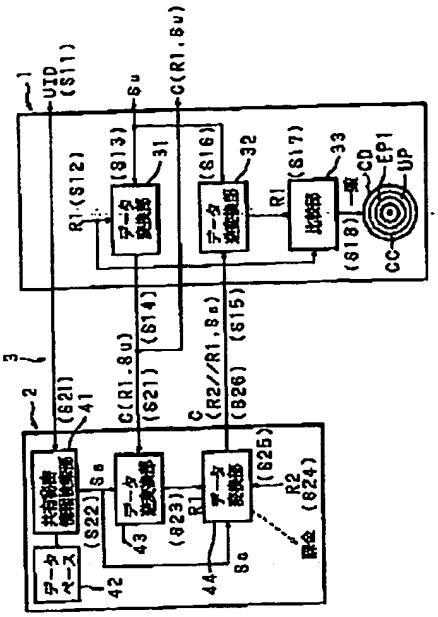
(54) ELECTRONIC INFORMATION DISTRIBUTION METHOD AND RECORDING MEDIUM

(57) Abstract

PROBLEM TO BE SOLVED: To reduce the burden of a server by starting a restoration program when the restored 1st information is matched with its own generated 1st information.

SOLUTION: A server device 2 generates the new random information (random number) R2 via an execution program EP2 and converts the data obtained by adding a random number R1 acquired at a data inverse conversion part 4 to the number R2 via a data conversion part 44 based on the shared secret information Ss that is read out of a database 42 and registered to generate the data C (R2/R1, Ss) which are sent to a user device 1. The device 1 makes an execution program EP1 perform the inverse conversion of the shared secret information that is previously inputted by a user himself via a data inverse conversion part 32 and acquires the number R1. Then the program EP1 compares the number R1 obtained at the part 32 with the previously generated number R1 via a comparator 33. When they are matched with each other its own thawing program UP is started to start the thawing of the compressed contents CC.

31. May 1999


1
UID (S11)
6u
C(R1.8u)
R1 (S12)
(S13)
31
(S16)
32
R1
(S17)
33
CD
EP1
UP
(S18)
CC
(S14)
(S15)
3
2
(S21)
41
C(R1.8u)
(S21)
C
(R2//R1.8u)
(S26)
(S22)
8a
43
(S23)
R1
(S25)
R2
(S24)
42
44
8a

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－39262

(43)公開日　平成11年(1999)２月12日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｚ
	9/06	５５０		9/06	５５０Ｚ
	12/14	３２０		12/14	３２０Ａ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｆ
					６６０Ｄ

審査請求　未請求　請求項の数12　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願平9－196212

(22)出願日　平成９年(1997)７月22日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　松本　達郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　磯道　宏世
東京都港区海岸３丁目９番15号　株式会社ジー・サーチ内

(74)代理人　弁理士　河野　登夫

最終頁に続く

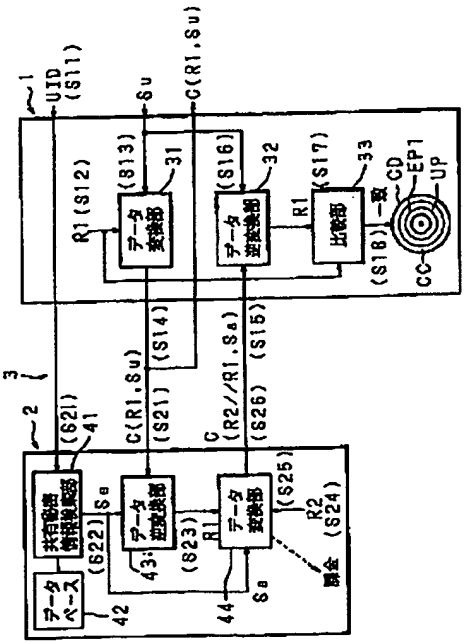
(54)【発明の名称】　電子情報配布方法及び記録媒体

(57)【要約】

【課題】　電子情報（コンテンツ）そのものはなんらかの加工（たとえば圧縮等）を加えた上で従来同様にCD-ROM等の記録媒体で予め配布しておき、加工された電子情報を復元するための情報を通信回線を介して送信することにより、膨大なデータ量にもなりうる電子情報を通信回線を介して送受する危険性を回避し得るようにする。

【解決手段】　ユーザ側装置１またはサーバ側装置２において発生された乱数を双方で共有する共有秘密情報（たとえばパスワード等）で暗号化して交換し、自身で発生して送信した乱数が戻ってきた場合にのみ相互を認証して圧縮されたコンテンツCCの復元を開始する。

本発明方法の第１の原理を説明するための模式図



1

【特許請求の範囲】

【請求項1】　配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、前記復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布する電子情報配布方法において、

前記ユーザ側装置は、第1の情報をランダムに発生し、この第1の情報に前記管理側装置で逆加工可能な第1の加工を施すことにより第2の情報を生成し、この第2の情報を前記管理側装置へ送信し、

前記管理側装置は、前記ユーザ側装置から受信した第2の情報に前記第1の加工の逆加工を施すことにより第1の情報を復元し、この復元した第1の情報に前記ユーザ側装置で逆加工可能な第2の加工を施すことにより第3の情報を生成し、この第3の情報を前記ユーザ側装置へ送信し、

前記ユーザ側装置は、前記管理側装置から受信した第3の情報に前記第2の加工の逆加工を施すことにより第1の情報を復元し、この復元された第1の情報を自身が発生した前記第1の情報と比較し、両者が一致している場合に前記復元プログラムを起動させることにより前記加工済み電子情報を復元することを特徴とする電子情報配布方法。

【請求項2】　配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、前記復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布する電子情報配布方法において、

前記管理側装置は、第1の情報をランダムに発生し、この第1の情報を前記ユーザ側装置へ送信し、

前記ユーザ側装置は、第2の情報をランダムに発生し、このランダムに発生した第2の情報と前記管理側装置から受信した第1の情報に前記管理側装置で逆加工可能な第1の加工を施すことにより第3の情報を生成し、この第3の情報を前記管理側装置へ送信し、

前記管理側装置は、前記ユーザ側装置から受信した第3の情報に前記第1の加工の逆加工を施すことにより第1の情報と第2の情報とを復元し、復元された第1の情報を自身が発生した前記第1の情報と比較し、両者が一致している場合に復元した第2の情報に前記ユーザ側装置で逆加工可能な第2の加工を施すことにより第4の情報を生成し、この第4の情報を前記ユーザ側装置へ送信し、

前記ユーザ側装置は、前記管理側装置から受信した第4

2

の情報に前記第2の加工の逆加工を施すことにより第2の情報を復元し、この復元された第2の情報を自身が発生した前記第2の情報と比較し、両者が一致している場合に前記復元プログラムを起動させることにより前記加工済み電子情報を復元することを特徴とする電子情報配布方法。

【請求項3】　前記管理側装置は、前記第1の情報を前記共有情報を使用して加工し、前記ユーザ側装置へ送信し、

前記ユーザ側装置は、前記管理側装置から受信した加工済みの第1の情報を外部に一旦提示し、提示された情報が再入力された場合に、前記第1の加工を施すことを特徴とする請求項2に記載の電子情報配布方法。

【請求項4】　配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、前記復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布する電子情報配布方法において、

前記ユーザ側装置は、前記電子情報に固有の第1の情報と前記ユーザ側装置と前記管理側装置とで予め共有している共有情報とを使用してパラメータを生成し、このパラメータに基づいて前記ユーザ側装置に関係する固有の第2の情報に第1の加工を施すことにより第3の情報を生成し、この第3の情報を前記管理側装置へ送信し、

前記管理側装置は、前記第1の情報と前記共有情報とから前記パラメータを生成し、前記ユーザ側装置から受信した第3の情報を前記パラメータを使用して前記第1の加工の逆加工を施すことにより前記第2の情報を復元し、この復元した第2の情報に前記パラメータを使用して第2の加工を施すことにより第4の情報を生成し、この第4の情報を前記ユーザ側装置へ送信し、

前記ユーザ側装置は、前記管理側装置から受信した第4の情報に前記パラメータを使用して前記第2の加工の逆加工を施すことにより第2の情報を復元し、この復元された第2の情報を前記ユーザ側装置に関係する前記固有の第2の情報と比較し、両者が一致している場合に前記復元プログラムを起動させることにより前記加工済み電子情報を復元することを特徴とする電子情報配布方法。

【請求項5】　前記ユーザ側装置に関係する固有の第2の情報は、ユーザ識別用の情報，ユーザ側装置固有の情報またはそのオペレーティングシステム固有の情報のいずれか一つまたは複数であることを特徴とする請求項4に記載の電子情報配布方法。

【請求項6】　配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して

管理側装置から指示を与えることにより、前記復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するためのユーザ側装置で使用されるプログラムが記録された記録媒体であって、

第1の情報をランダムに発生させるステップと、

前記第1の情報に前記管理側装置で逆加工可能な第1の加工を施すことにより第2の情報を生成させるステップと、

前記第2の情報を前記管理側装置へ送信させるステップと、

前記管理側装置が、前記ユーザ側装置から受信した第2の情報を前記第1の加工の逆加工を施すことにより復元した第1の情報に前記ユーザ側装置で逆加工可能な第2の加工を施すことにより生成して送信した第4の情報を受信させるステップと、

前記管理側装置から受信した第4の情報に前記第2の加工の逆加工を施すことにより第1の情報を復元させるステップと、

復元された第1の情報を自身が発生した前記第1の情報と比較させるステップと、

両者の比較結果が一致している場合に前記復元プログラムを起動させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする記録媒体。

【請求項7】　配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、前記復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するための管理側装置で使用されるプログラムが記録された記録媒体であって、

前記ユーザ側装置が、ランダムに発生した第1の情報に前記管理側装置で逆変換可能な第1の加工を施すことにより生成して送信した第2の情報を受信させるステップと、

受信した第2の情報に前記第1の加工の逆加工を施すことにより第1の情報を復元させるステップと、

復元した第1の情報に前記ユーザ側装置で逆加工可能な第2の加工を施すことにより第4の情報を生成させるステップと、

前記第4の情報を前記ユーザ側装置へ送信させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする記録媒体。

【請求項8】　配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して

管理側装置から指示を与えることにより、前記復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するためのユーザ側装置で使用されるプログラムが記録された記録媒体であって、

前記管理側装置が、ランダムに発生して送信した第1の情報を受信させるステップと、

第2の情報をランダムに発生させるステップと、

前記ランダムに発生した第2の情報と前記管理側装置から受信した第1の情報とに前記管理側装置で逆加工可能な第1の加工を施すことにより第3の情報を生成させるステップと、

前記第3の情報を前記管理側装置へ送信させるステップと、

前記管理側装置が、前記ユーザ側装置から受信した第3の情報に前記第1の加工の逆加工を施すことにより第1の情報と第2の情報とを復元し、復元した第1の情報を自身が発生した前記第1の情報と比較し、両者が一致している場合に復元した第2の情報に前記ユーザ側装置で逆加工可能な第2の加工を施すことにより生成して送信した第4の情報を受信させるステップと、

受信した第4の情報に前記第2の加工の逆加工を施すことにより第2の情報を復元させるステップと、

復元された第2の情報を自身が発生した前記第2の情報と比較するステップと、

両者の比較結果が一致している場合に前記復元プログラムを起動させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする記録媒体。

【請求項9】　配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、前記復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するための管理側装置で使用されるプログラムが記録された記録媒体であって、

第1の情報をランダムに発生させるステップと、

前記第1の情報を前記ユーザ側装置へ送信させるステップと、

前記ユーザ側装置で、ランダムに発生した第2の情報と前記管理側装置から受信した第1の情報とに前記管理側装置で逆加工可能な第1の加工を施すことにより生成して送信した第3の情報を受信させるステップと、

ユーザ側装置から受信した第3の情報に前記第1の加工の逆加工を施すことにより第1の情報と第2の情報とを復元させるステップと、

復元された第1の情報を自身が発生した前記第1の情報と比較するステップと、

両者の比較結果が一致している場合に復元した第２の情報に前記ユーザ側装置で逆加工可能な第２の加工を施すことにより第４の情報を生成させるステップと、
前記第４の情報を前記ユーザ側装置へ送信させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする記録媒体。

【請求項１０】　配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、前記復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するためのユーザ側装置で使用されるプログラムが記録された記録媒体であって、
前記電子情報に固有の第１の情報とこの第１の情報と前記ユーザ側装置と前記管理側装置とで予め共有している共有情報とを使用してパラメータを生成させるステップと、
前記パラメータに基づいて前記ユーザ側装置に関係する固有の第２の情報に第１の加工を施すことにより第３の情報を生成させるステップと、
前記第３の情報を前記管理側装置へ送信させるステップと、
前記管理側装置が、前記ユーザ側装置から受信した第３の情報に前記第１の情報と前記共有情報とから生成した前記パラメータを使用して前記第１の加工の逆加工を施すことにより前記第２の情報を復元し、この復元した第２の情報に前記パラメータを使用して第２の加工を施すことにより生成して送信した第４の情報を受信させるステップと、
受信した第４の情報に前記パラメータを使用して前記第２の加工の逆加工を施すことにより第２の情報を復元させるステップと、
復元された第２の情報を前記ユーザ側装置に関係する前記固有の第２の情報と比較するステップと、
両者の比較結果が一致している場合に前記復元プログラムを起動させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする記録媒体。

【請求項１１】　配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、前記復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するための管理側装置で使用されるプログラムが記録された記録媒体であって、
前記ユーザ側装置が、前記電子情報に固有の第１の情報

と前記ユーザ側装置と前記管理側装置とで予め共有している共有情報とを使用して生成したパラメータに基づいて前記ユーザ側装置に関係する固有の第２の情報に第１の加工を施すことにより生成して送信した第３の情報を受信させるステップと、
前記第１の情報と前記共有情報とから前記パラメータを生成させるステップと、
前記ユーザ側装置から受信した第３の情報を前記パラメータを使用して前記第１の加工の逆加工を施すことにより前記第２の情報を復元させるステップと、
復元した第２の情報に前記パラメータを使用して第２の加工を施すことにより第４の情報を生成させるステップと、
前記第４の情報を前記ユーザ側装置へ送信させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする記録媒体。

【請求項１２】　前記ユーザ側装置に関係する固有の第２の情報は、ユーザ識別用の情報，ユーザ側装置固有の情報またはそのオペレーティングシステム固有の情報のいずれか一つまたは複数であることを特徴とする請求項１０又は１１のいずれかに記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンテンツ、具体的にはソフトウェア，画像データ等のデジタルをCD-ROM，フレキシブルディスク等の記録媒体に記録した状態で配布する方法に関する。

【０００２】

【従来の技術】一般的にコンテンツと称されるソフトウェア，画像等の電子情報はCD-ROM，フレキシブルディスク等の記録媒体に記録した状態で通常は有料で販売されるが、無料で配布される場合もある。また近年では、コンテンツを圧縮化，暗号化等のデータ変換（加工）を行なった上で記録した記録媒体をまず無料で配布しておき、希望者にのみ逆データ変換のための情報を与えることによりその使用を可能にするというような方法も採られる。この際、逆データ変換のための情報を有料とする場合と無料とする場合との両方があり得るが、いずれにしろそのような情報のセキュリティが必要になる。

【０００３】更に、上述のような情報を通信回線を介して送受する場合には、しかも有料である場合には、当然のことながら双方の身元確認（認証）が必要になり、これに伴ってID，パスワード等のセキュリティも同時に必要になる。

【０００４】このような事情から、従来はたとえば、図15または図16の模式図に示されているような手法が採用されいた。なお、いずれの例においても、ユーザ側装置１とはコンテンツの利用を希望するユーザが使用するコンピュータシステムを、サーバ側装置２とはコンテンツを有料で販売または無料で配布する組織のコンピュータ

システムである。

【0005】まず、図15を参照して、従来技術の一例について説明する。但し、この例では、コンテンツC自体はユーザの手元にはなく、通信回線3を介してサーバ側装置2から暗号化されて送信される。

【0006】図15において、ユーザ側装置1では、まずユーザが自身の識別符号（以下、ユーザIDと言う）UIDとパスワードPWu とを自身で入力して通信回線3を介してサーバ側装置2へ送信させる。

【0007】サーバ側装置2では、ユーザ側装置1からユーザID UIDとパスワードPWu とを通信回線3を介して受信すると、パスワード検索部21が ID/パスワードデータベース22に予め登録されて蓄積されている複数のユーザのユーザIDを検索させて登録済みのパスワードの中から対応するパスワードPWc を取り出す。そして、サーバ側装置2では、受信したユーザのパスワードPWu と ID/パスワードデータベース22から取り出した登録済みのパスワードPWc とを比較部23が比較し、一致検出を行なう。

【0008】比較部23による比較の結果、両者が一致した場合には、暗号化部24がコンテンツCを登録済みのパスワードPWc で暗号化し、連結部25が暗号化部24により暗号化されたコンテンツE(C, PWc) に復号化プログラムPを連結し、その結果として得られる送信データP+E(C, PWc) をユーザ側装置1へ通信回線3を介して送信させる。

【0009】この送信データP+E(C, PWc) を受信したユーザ側装置1では、復号化部11が先にユーザ自身が入力したパスワードPWc で送信データP+E(C, PWc) を復号し、その結果得られる復号プログラムPによりコンテンツCを得る。

【0010】次に、図16を参照して、従来技術の他の例について説明する。但し、この例では、コンテンツCが暗号化されたコンテンツ（以下、暗号化コンテンツと言う）E(C, Key) 自体が予めCD-ROM等の記録媒体に記録された状態でユーザの手元に配布されており、通信回線3を介してサーバ側装置2から復号化のためのキーが送信される。ユーザ側装置1ではこのサーバ側装置2から送信されてくるキーで手元の暗号化コンテンツE(C, Key) を復号化する。

【0011】図16において、ユーザ側装置1では、まずユーザが自身のユーザID UIDとパスワードPWu と予め入手しているCD-ROM等の記録媒体のラベル等に記載されているコンテンツID C-ID とを入力して通信回線3を介してサーバ側装置2へ送信させる。

【0012】サーバ側装置2では、ユーザ側装置1からユーザID UIDとパスワードPWu とを通信回線3を介して受信すると、パスワード検索部21が ID/パスワードデータベース22に予め登録されて蓄積されている複数のユーザのユーザIDを検索して登録済みのスワードの中から対応するパスワードPWc を取り出す。そしてサーバ側装置2では、受信したユーザのパスワードPWu と ID/パスワードデータベース22から取り出した登録済みのパスワードPWc とを比較部23が比較し、一致検出を行なう。

【0013】比較部23による比較の結果、ユーザ側装置1から受信したパスワードPWu と ID/パスワードデータベース22から読み出した登録済みパスワードPWc とが一致した場合には、暗号化部24がコンテンツID C-ID に対応るう復号化キーKey を登録済みパスワードPWc で暗号化し、連結部25が暗号化部24により暗号化された復号化キーE(Key, PWc) を送信データとしてユーザ側装置1へ通信回線3を介して送信する。

【0014】この送信データとしての復号化キーE(Key, PWc) を受信したユーザ側装置1では、第1復号化部111 が先にユーザ自身が入力したパスワードPWu で復号化キーE(Key, PWc) を復号して復号化キーKey を得る。そして、この復号化キーKey を使用して、既に入手済みの暗号化されたコンテンツE(C, Key) を第2復号化部112 が復号することにより、最終的にコンテンツCを得る。

【0015】なお、上述のいずれの例においても、コンテンツCが有料である場合には、サーバ側装置2において適宜のタイミングで課金のための処理を行なうことが可能である。

【0016】

【発明が解決しようとする課題】上述の第1の従来例では、サーバ側においてユーザのパスワードでコンテンツを暗号化してユーザ側へ送信するため、その都度、コンテンツを暗号化する必要があり、サーバ側での負担が大きい。また、暗号化されたコンテンツが通信回線を介して送信されるため、通信コストが大きくなり、更に通信中にエラーが生じてユーザ側で完全なコンテンツを受信出来ない虞もある。また更に、ユーザ側からサーバ側へパスワードが平文で送信されるため、漏洩の虞がある。

【0017】また、上述の第2の従来例では、サーバ側でコンテンツ毎の復号化キーを管理する必要がある。またこの復号化キーが漏洩した場合には防御策がなく、コンテンツ自体は暗号化されているとはいえそれを記録した記録媒体が予め無料で配布されているため、多額の損失が生じる虞がある。また、ユーザに予め配布するコンテンツにそれを識別するための情報（コンテンツID）を付加しておく必要がある。更に、ユーザ側からサーバ側へパスワードが平文で送信されるため、漏洩の虞がある。

【0018】本発明はこのような事情に鑑みてなされたものであり、電子情報（コンテンツ）そのものはなんらかの加工（たとえば圧縮等）を加えた上で従来同様にCD-ROM等の記録媒体で予め配布しておき、加工された電子情報を復元するための情報を通信回線を介して送信する。これにより、膨大なデータ量にもなりうる電子情報を通信回線を介して送受する危険性を回避し得る。

【0019】また、ユーザ側装置またはサーバ側装置において発生された乱数を双方で共有する共有秘密情報（たとえばパスワード等）で暗号化して交換し、自身で発生して送信した乱数が戻ってきた場合にのみ相互を認証して電子情報の復元を開始するようにする。これにより、相互の認証がより厳密に行なえるようになる。

【0020】更に、ユーザ側装置で発生させた乱数を共有秘密情報で暗号化してサーバ側装置へ送信し、サーバ側装置は共有秘密情報で暗号を解読し、再度共有秘密情報で乱数を暗号化してユーザ側装置へ送信する。これをユーザ側装置で再度共有秘密情報で解読し、得られた乱数が自身がサーバ側装置へ送信した乱数である場合には電子情報の復元を開始する。これにより、相互に認証がより厳密に行なえると共に、電子情報を復元するための情報が漏洩することがない。

【0021】また更に、サーバ側装置で生成した乱数をユーザ側装置へ送信し、ユーザ側装置では自身で生成した乱数と合わせて共有秘密情報で暗号化してユーザ側装置へ送信する。サーバ側装置では、共有秘密情報で暗号を解読し、サーバ側装置で生成して送信した乱数が得られればユーザ側装置を正規のユーザと認証する。また、サーバ側装置はこの際にユーザ側装置で生成して送信してきた乱数も取り出し、それに何らかのランダムな情報を加えて共有秘密情報で暗号化してユーザ側装置へ送信する。ユーザ側装置では、共有秘密情報により暗号を解読し、得られた乱数が自身で生成して送信した乱数であれば、電子情報の復元を開始する。これにより、相互に認証がより厳密に行なえると共に、電子情報を復元するための情報が漏洩することがない。

【0022】更にまた、ユーザ側装置とサーバ側装置との双方で電子情報に固有な情報と共有秘密情報とから暗号化／復号化のキーを生成し、ユーザ側装置からユーザ側装置に関係する情報（たとえば、ユーザID，ハードウェアのID，オペレーティングシステムのID等）を暗号化してサーバ側装置へ送信する。サーバ側装置では、キーにより暗号を解読し、ユーザ側装置に関係する情報を取り出す。更に、サーバ側装置はユーザ側装置に関係する情報に自身で発生した乱数を加えて暗号化しげユーザ側装置へ送信する。ユーザ側装置では、暗号を解読して得られた結果が自身が発生してサーバ側装置へ送信した情報であれば、電子情報の復元を開始する。これにより、相互に認証がより厳密に行なえると共に、電子情報を復元するための情報が漏洩することがない。

【0023】

【課題を解決するための手段】本発明は、配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布する電子情報配布方法であって、ユーザ側装置は、第１の情報をランダムに発生し、この第１の情報に管理側装置で逆加工可能な第１の加工を施すことにより第２の情報を生成し、この第２の情報を管理側装置へ送信し、管理側装置は、ユーザ側装置から受信した第２の情報に第１の加工の逆加工を施すことにより第１の情報を復元し、この復元した第１の情報にユーザ側装置で逆加工可能な第２の加工を施すことにより第３の情報を生成し、この第３の情報をユーザ側装置へ送信し、ユーザ側装置は、管理側装置から受信した第３の情報に第２の加工の逆加工を施すことにより第１の情報を復元し、この復元された第１の情報を自身が発生した第１の情報と比較し、両者が一致している場合に復元プログラムを起動させることにより加工済み電子情報を復元することを特徴とする。

【0024】また本発明は、配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布する電子情報配布方法であって、管理側装置は、第１の情報をランダムに発生し、この第１の情報をユーザ側装置へ送信し、ユーザ側装置は、第２の情報をランダムに発生し、このランダムに発生した第２の情報と管理側装置から受信した第１の情報に管理側装置で逆加工可能な第１の加工を施すことにより第３の情報を生成し、この第３の情報を管理側装置へ送信し、管理側装置は、ユーザ側装置から受信した第３の情報に第１の加工の逆加工を施すことにより第１の情報と第２の情報とを復元し、復元された第１の情報を自身が発生した第１の情報と比較し、両者が一致している場合に復元した第２の情報にユーザ側装置で逆加工可能な第２の加工を施すことにより第４の情報を生成し、この第４の情報をユーザ側装置へ送信し、ユーザ側装置は、管理側装置から受信した第４の情報に第２の加工の逆加工を施すことにより第２の情報を復元し、この復元された第２の情報を自身が発生した第２の情報と比較し、両者が一致している場合に復元プログラムを起動させることにより加工済み電子情報を復元することを特徴とする。

【0025】また本発明は、上述の電子情報配布方法において、管理側装置が、第１の情報を共有情報を使用して加工し、ユーザ側装置へ送信し、ユーザ側装置が、管理側装置から受信した加工済みの第１の情報を外部に一旦提示し、提示された情報が再入力された場合に、第１の加工を施すことを特徴とする。

【0026】また本発明は配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情

報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布する電子情報配布方法であって、ユーザ側装置は、電子情報に固有の第1の情報とユーザ側装置と管理側装置とで予め共有している共有情報とを使用してパラメータを生成し、このパラメータに基づいてユーザ側装置に関係する固有の第2の情報に第1の加工を施すことにより第3の情報を生成し、この第3の情報を管理側装置へ送信し、管理側装置は、第1の情報と共有情報とからパラメータを生成し、ユーザ側装置から受信した第3の情報をパラメータを使用して第1の加工の逆加工を施すことにより第2の情報を復元し、この復元した第2の情報にパラメータを使用して第2の加工を施すことにより第4の情報を生成し、この第4の情報をユーザ側装置へ送信し、ユーザ側装置は、管理側装置から受信した第4の情報にパラメータを使用して第2の加工の逆加工を施すことにより第2の情報を復元し、この復元された第2の情報をユーザ側装置に関係する固有の第2の情報と比較し、両者が一致している場合に復元プログラムを起動させることにより加工済み電子情報を復元することを特徴とする。

【0027】また本発明に係る電子情報配布方法は、上述の発明において、ユーザ側装置に関係する固有の第2の情報は、ユーザ識別用の情報，ユーザ側装置固有の情報またはそのオペレーティングシステム固有の情報のいずれか一つまたは複数であることを特徴とする。

【0028】また本発明に係る記録媒体は、配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するためのユーザ側装置で使用されるプログラムが記録された記録媒体であって、第1の情報をランダムに発生させるステップと、第1の情報に管理側装置で逆加工可能な第1の加工を施すことにより第2の情報を生成させるステップと、第2の情報を管理側装置へ送信させるステップと、管理側装置が、ユーザ側装置から受信した第2の情報を第1の加工の逆加工を施すことにより復元した第1の情報にユーザ側装置で逆加工可能な第2の加工を施すことにより生成して送信した第4の情報を受信させるステップと、管理側装置から受信した第4の情報に第2の加工の逆加工を施すことにより第1の情報を復元させるステップと、復元された第1の情報を自身が発生した第1の情報と比較させるステップと、両者の比較結果が一致している場合に復元プログラムを起動させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする。

【0029】本発明に係る記録媒体は、配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するための管理側装置で使用されるプログラムが記録された記録媒体であって、ユーザ側装置が、ランダムに発生した第1の情報に管理側装置で逆変換可能な第1の加工を施すことにより生成して送信した第2の情報を受信させるステップと、受信した第2の情報に第1の加工の逆加工を施すことにより第1の情報を復元させるステップと、復元した第1の情報にユーザ側装置で逆加工可能な第2の加工を施すことにより第4の情報を生成させるステップと、第4の情報をユーザ側装置へ送信させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする。

【0030】また本発明に係る記録媒体は、配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するためのユーザ側装置で使用されるプログラムが記録された記録媒体であって、管理側装置が、ランダムに発生して送信した第1の情報を受信させるステップと、第2の情報をランダムに発生させるステップと、ランダムに発生した第2の情報と管理側装置から受信した第1の情報とに管理側装置で逆加工可能な第1の加工を施すことにより第3の情報を生成させるステップと、第3の情報を管理側装置へ送信させるステップと、管理側装置が、ユーザ側装置から受信した第3の情報に第1の加工の逆加工を施すことにより第1の情報と第2の情報とを復元し、復元した第1の情報を自身が発生した第1の情報と比較し、両者が一致している場合に復元した第2の情報にユーザ側装置で逆加工可能な第2の加工を施すことにより生成して送信した第4の情報を受信させるステップと、受信した第4の情報に第2の加工の逆加工を施すことにより第2の情報を復元させるステップと、復元された第2の情報を自身が発生した第2の情報と比較するステップと、両者の比較結果が一致している場合に復元プログラムを起動させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする。

【0031】また本発明に係る記録媒体は、配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プロ

グラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するための管理側装置で使用されるプログラムが記録された記録媒体であって、第1の情報をランダムに発生させるステップと、第1の情報をユーザ側装置へ送信させるステップと、ユーザ側装置で、ランダムに発生した第2の情報と管理側装置から受信した第1の情報とに管理側装置で逆加工可能な第1の加工を施すことにより生成して送信した第3の情報を受信させるステップと、ユーザ側装置から受信した第3の情報に第1の加工の逆加工を施すことにより第1の情報と第2の情報とを復元させるステップと、復元された第1の情報を自身が発生した第1の情報と比較するステップと、両者の比較結果が一致している場合に復元した第2の情報にユーザ側装置で逆加工可能な第2の加工を施すことにより第4の情報を生成させるステップと、第4の情報をユーザ側装置へ送信させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする。

【0032】また本発明に係る記録媒体は、配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プログラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するためのユーザ側装置で使用されるプログラムが記録された記録媒体であって、電子情報に固有の第1の情報とこの第1の情報とユーザ側装置と管理側装置とで予め共有している共有情報とを使用してパラメータを生成させるステップと、パラメータに基づいてユーザ側装置に関係する固有の第2の情報に第1の加工を施すことにより第3の情報を生成させるステップと、第3の情報を管理側装置へ送信させるステップと、管理側装置が、ユーザ側装置から受信した第3の情報に第1の情報と共有情報とから生成したパラメータを使用して第1の加工の逆加工を施すことにより第2の情報を復元し、この復元した第2の情報にパラメータを使用して第2の加工を施すことにより生成して送信した第4の情報を受信させるステップと、受信した第4の情報にパラメータを使用して第2の加工の逆加工を施すことにより第2の情報を復元させるステップと、復元された第2の情報をユーザ側装置に関係する固有の第2の情報と比較するステップと、両者の比較結果が一致している場合に復元プログラムを起動させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする。

【0033】また本発明に係る記録媒体は、配布すべき電子情報に所定の加工を施した加工済み電子情報と、この加工済み電子情報を加工前の状態に復元する復元プロ

グラムとが記録された記録媒体の読み取りが可能なユーザ側装置に通信回線を介して管理側装置から指示を与えることにより、復元プログラムを起動して加工済み電子情報を元の電子情報に復元することにより電子情報を配布するための管理側装置で使用されるプログラムが記録された記録媒体であって、ユーザ側装置が、電子情報に固有の第1の情報とユーザ側装置と管理側装置とで予め共有している共有情報とを使用して生成したパラメータに基づいてユーザ側装置に関係する固有の第2の情報に第1の加工を施すことにより生成して送信した第3の情報を受信させるステップと、第1の情報と共有情報とからパラメータを生成させるステップと、ユーザ側装置から受信した第3の情報をパラメータを使用して第1の加工の逆加工を施すことにより第2の情報を復元させるステップと、復元した第2の情報にパラメータを使用して第2の加工を施すことにより第4の情報を生成させるステップと、第4の情報をユーザ側装置へ送信させるステップとを含むコンピュータ読み取り可能なプログラムを記録したことを特徴とする。

【0034】また本発明に係る記録媒体は、上述の記録媒体において、ユーザ側装置に関係する固有の第2の情報は、ユーザ識別用の情報，ユーザ側装置固有の情報またはそのオペレーティングシステム固有の情報のいずれか一つまたは複数であることを特徴とする。

【0035】

【発明の実施の形態】以下、本発明をその実施の形態を示す図面に基づいて詳述するが、まず最初に本発明の電子情報配布方法（以下、本発明方法という）を実施するためのシステム構成を説明し、次に本発明方法の原理について説明し、その後に実際の実施の形態について説明する。

【0036】図1は本発明方法の実施に使用されるシステム構成の一例を示す模式図である。図1において、参照符号1は本発明方法により有料または無料で配布される電子情報（以下、コンテンツと言う）を利用するユーザが使用するコンピュータシステム（以下、ユーザ側装置と言う）を示しており、参照符号2はそのコンテンツCを有料または無料で配布する業者が自身で、または他の業者に委託して運営する管理側装置を示している。なお、ユーザ側装置1とサーバ側装置2とはたとえば一般の公衆電話回線等の通信回線3で接続されており、いわゆるコンピュータ通信が可能である。

【0037】ユーザ側装置1は、大きくは本体111，ディスプレイ112 及び入力操作手段（キーボード113，マウス114 等）で構成されている。本体111 には、通常のコンピュータシステムと同様に、ハードディスクドライブ(HDD)111，フレキシブルディスクドライブ(FDD)115，CD-ROMドライブ116 及び図示されていないCPU，RAM，ROM等が備えられている。

【0038】CD-ROMドライブ116 にはCD-ROM CD が装入

されるが、このCD-ROM CD には本発明方法により配布されるコンテンツCをたとえば圧縮加工したデジタルデータCCとその解凍用のプログラムUPと、更に本発明方法の実行に必要なプログラム（以下、実行プログラムと言う）EP1とが記録されている。なお、FDD115にはフレキシブルディスクFDが装入されるが、このフレキシブルディスクFDにコンテンツCをたとえば圧縮加工したデジタルデータCCとその解凍用のプログラムUPと、更に実行プログラムEP1 とを記録しておいてもよく、またCD-ROM CD, フレキシブルディスクFD以外の記録媒体を利用することも勿論可能である。

【００３９】いずれにしろ、記録媒体に記録されているコンテンツCをたとえば圧縮加工したデジタルデータCCとその解凍用のプログラムUPと、更に実行プログラムEP1 とは本体110 のHDD111に一旦記憶されてから実際に使用される。

【００４０】一方、サーバ側装置２も基本的には一般的なコンピュータシステムであり、HDD211が備えられており、このHDD211には本発明方法の実行に必要な実行プログラムEP2 がたとえばCD-ROM CD 等の記録媒体からインストールされて記憶されている。

【００４１】図２は本発明方法の第１の原理を説明するための模式図、図３はそのユーザ側装置１の動作手順を示すフローチャート、図４はサーバ側装置２の動作手順を示すフローチャートである。

【００４２】なお、以下の各原理説明においては、コンテンツC自体は自己解凍型のソフトウェアとして圧縮されたデジタルデータCCの状態でCD-ROM CD に記録されてユーザの手元に予め無料で配布されており、このCD-ROM CD には更に圧縮されたデジタルデータCCを自己解凍するための解凍プログラムUPと、この解凍プログラムUPを起動させるための処理を実行するユーザ側装置１用の実行プログラムEP1 とが記録されている。また、ユーザ側装置１において実際に動作するのは実行プログラムEP1 であり、サーバ側装置２において実際に動作するのは実行プログラムEP2 である。

【００４３】図２において、ユーザ側装置１では、まずユーザが自身のユーザ識別番号（以下、ユーザIDと言う）UIDを入力すると、それを実行プログラムEP1 が通信回線３を介してサーバ側装置２へ送信させる（ステップS11）。また同時に、ユーザは共有秘密情報Suをユーザ側装置１に入力する。この共有秘密情報Suが入力されると、実行プログラムEP1 はランダム情報（乱数）R1を発生させ（ステップS12）、この乱数R1を共有秘密情報Suをパラメータとしてデータ変換部31にデータ変換を施させることによりデータC(R1, Su) を生成し（ステップS13）、ユーザに提示する。

【００４４】このようにして実行プログラムEP1 が提示したデータC(R1, Su) をユーザが再度ユーザ側装置１に入力することにより、実行プログラムEP1 はそれを通信回線３を介してサーバ側装置２へ送信させる（ステップS14）。

【００４５】サーバ側装置２では、ユーザ側装置１からユーザID UID及びデータC(R1, Su)を通信回線３を介して受信すると（ステップS21）、実行プログラムEP2 が共有秘密情報検索部41にデータベース42に予め登録されて蓄積されている複数のユーザのユーザID UIDを検索させて登録済みの共有秘密情報の中から対応する登録済みの共有秘密情報Ssを取り出させる（ステップS22）。そして実行プログラムEP2 は、受信したデータC(R1, Su) をデータベース42から取り出した登録済みの共有秘密情報Ssでデータ逆変換部43に逆変換させて乱数R1を得る（ステップS23）。

【００４６】次にサーバ側装置２では、実行プログラムEP2 が新たにランダム情報（乱数）R2を発生させ（ステップS24）、データ逆変換部43により得られた乱数R1と乱数R2とを合わせたデータをデータベース42から読み出した登録済みの共有秘密情報Ssを使用してデータ変換部44に変換させてデータC(R2//R1, Ss) を生成し（ステップS25）、通信回線３を介してユーザ側装置１へ送信させる（ステップS26）。

【００４７】なお、データ変換部44でこのデータC(R2//R1, Ss) を生成する時点で、課金処理が必要であれば実行する。

【００４８】このデータC(R2//R1, Ss) を受信すると（ステップS15）、ユーザ側装置１では、実行プログラムEP1 がデータ逆変換部32に先にユーザ自身が入力した共有秘密情報Suで逆変換させることにより、乱数R1を得る（ステップS16）。実行プログラムEP1 は、このデータ逆変換部32で得られた乱数R1を先に自身が発生させた乱数R1と比較部33で比較し（ステップS17）、一致していれば自己解凍プログラムUPを起動して圧縮されているコンテンツCCの解凍を開始させる（ステップS18）。

【００４９】図５は本発明方法の第２の原理を説明するための模式図、図６はそのユーザ側装置１の動作手順を示すフローチャート、図７はサーバ側装置２の動作手順を示すフローチャートである。

【００５０】ユーザ側装置１では、まずユーザが自身のユーザID UIDを入力すると、それを実行プログラムEP1 が通信回線３を介してサーバ側装置２へ送信させる（ステップS31）。

【００５１】これに対して、サーバ側装置２はユーザ側装置１からユーザID UIDを受信すると（ステップS41）、ランダム情報（乱数）R1を発生させ（ステップS42）、通信回線３を介してユーザ側装置１へ送信させる（ステップS43）。ユーザ側装置１ではこの乱数R1を受信してユーザに提示する（ステップS32）。

【００５２】ユーザは、このサーバ側装置２から提示された乱数R1と共有秘密情報Suとをユーザ側装置１に入力する（ステップS33）。この乱数R1と共有秘密情報Suとが

入力されると、実行プログラムEP1 はランダム情報（乱数）R2を発生させ（ステップS34）、共有秘密情報Suをパラメータとしてデータ変換部31に乱数R1と乱数R2とを合わせてデータ変換を施させてデータC(R2//R1, Su) を生成させ（ステップS35）、ユーザに提示する。

【００５３】このようにして実行プログラムEP1 が提示したデータC(R2//R1, Su) をユーザが再度ユーザ側装置１に入力することにより、実行プログラムEP1 はそれを通信回線３を介してサーバ側装置２へ送信させる（ステップS36）。

【００５４】サーバ側装置２では、ユーザ側装置１からデータC(R2//R1, Su) を通信回線３を介して受信すると（ステップS44）、実行プログラムEP2 が先に受信しているユーザID UIDに従って共有秘密情報検索部41にデータベース42に予め登録されて蓄積されている複数のユーザのユーザID UIDを検索させて登録済みの共有秘密情報の中から対応する登録済みの共有秘密情報Ssを取り出させる（ステップS45）。そして実行プログラムEP2 は、受信したデータC(R2//R1, Su) をデータベース42から取り出された登録済みの共有秘密情報Ssでデータ逆変換部43に逆変換させて乱数R1, R2を得る（ステップS46）。

【００５５】次にサーバ側装置２では、実行プログラムEP2 がデータ逆変換部43が取り出した乱数R1を先にユーザ側装置１へ送信した乱数R1と比較部45に比較させ（ステップS47）、一致していれば、新たにランダム情報（乱数）R3を発生させ（ステップS48）、この乱数R3と先にデータ逆変換部43により得られた乱数R2とを合わせたデータをデータベース42から読み出した登録済みの共有秘密情報Ssを使用してデータ変換部44に変換させてデータC(R3//R2, Ss) を生成させ（ステップS49）、通信回線３を介してユーザ側装置１へ送信させる（ステップS50）。

【００５６】なお、データ変換部44でこのデータC(R3//R2, Ss) を生成する時点で、課金処理が必要であれば実行する。

【００５７】このデータC(R3//R2, Ss) を受信すると（ステップS37）、ユーザ側装置１では、実行プログラムEP1 がデータ逆変換部32に先にユーザ自身が入力した共有秘密情報Suで逆変換させることにより（ステップS38）、乱数R2を得る。実行プログラムEP1 は、このデータ逆変換部32で得られた乱数R2を先に自身が発生した乱数R2と比較部33に比較させ（ステップS39）、一致していれば自己解凍プログラムUPを起動して圧縮されているコンテンツCCの解凍を開始させる（ステップS40）。

【００５８】図８は本発明方法の第３の原理を説明するための模式図、図９はそのユーザ側装置１の動作手順を示すフローチャート、図10はサーバ側装置２の動作手順を示すフローチャートである。

【００５９】ユーザ側装置１では、まずユーザが自身のユーザID UIDを入力すると、それを実行プログラムEP1 が通信回線３を介してサーバ側装置２へ送信させる（ステップS51）。また同時に、ユーザは共有秘密情報Suをユーザ側装置１に入力する（ステップS52）。この共有秘密情報Suが入力されると、実行プログラムEP1 はコンテンツCの固有情報（以下、コンテンツ固有情報と言う）PIDをCD-ROM CD から読み出し（ステップS53）、これと共有秘密情報Suとから変換パラメータ生成部34に変換パラメータKYを生成させる（ステップS54）。

【００６０】次に、実行プログラムEP1 は、変換パラメータKYによって、ユーザUID とユーザ側装置１に固有のハードウェア固有情報、またはユーザ側装置１にインストールされているOS（オペレーティングシステム）固有の情報（以下、ハード／OS固有情報と言う）HIDを読み出し（ステップS55）、これとユーザID UIDとを合わせて変換パラメータKYによりデータ変換部31にデータ変換を施させてデータC(HID//UID, KY) を生成させ（ステップS56）、ユーザに提示する。

【００６１】このようにして実行プログラムEP1 が提示したデータC(HID/UID, KY)をユーザが再度ユーザ側装置１に入力することにより、実行プログラムEP1 はそれを通信回線３を介してサーバ側装置２へ送信させる（ステップS57）。

【００６２】サーバ側装置２では、ユーザ側装置１からデータC(HID/UID, KY)を通信回線３を介して受信すると（ステップS72）、実行プログラムEP2 が先に受信しているユーザID UIDに従って（ステップS71）、共有秘密情報検索部41にデータベース42に予め登録されて蓄積されている複数のユーザのユーザIDを検索させて登録済みの共有秘密情報の中から対応する登録済みの共有秘密情報Ssを取り出させる（ステップS73）。そして実行プログラムEP2 は、この共有秘密情報SsとコンテンツCの固有情報PID とから変換パラメータ生成部46にパラメータKYを生成させる（ステップS74）。

【００６３】次に、サーバ側装置２では、実行プログラムEP2 が、変換パラメータ生成部46が生成したパラメータKYを使用して、先にユーザ側装置１から受信しているデータC(HID/UID, KY)をデータ逆変換部43に逆変換させてデータHID//UIDを得る（ステップS75）。次に、実行プログラムEP2 は、データ逆変換部43が取り出したデータHID//UIDの内のデータUID を先に受信していたユーザID UIDと比較部45に比較させる（ステップS76）。

【００６４】なお、この比較部45でのユーザID UIDの比較の時点で、課金処理が必要であれば実行する。

【００６５】比較部45による比較結果が一致していれば、実行プログラムEP2 は新たにランダム情報（乱数）R2を発生させ（ステップS77）、この乱数R2と先にデータ逆変換部43により得られたデータHID//UIDの内のハード／OS固有情報HID とを先に変換パラメータ生成部46が生成した変換変換パラメータKYD でデータ変換部44に変換させてデータC(R2//HID, KY)を得る（ステップS78）。このデータ変換部44により得られたデータC(R2//HID, KY)

は通信回線3を介してサーバ側装置2へ送信される（ステップS79）。

【0066】このデータC(R2//HID, KY)を受信すると（ステップS58）、ユーザ側装置1では、実行プログラムEP1が、データC(R2//HID, KY)を先に変換パラメータ生成部34が生成した変換パラメータでデータ逆変換部32に逆変換させることにより、ハード／OS固有情報HIDを得る（ステップS51）。実行プログラムEP1は、このデータ逆変換部32で得られたハード／OS固有情報HIDをユーザ側装置1のハード／OS固有情報HIDと比較部33に比較させ（ステップS60）、一致していれば自己解凍プログラムUPを起動して圧縮されているコンテンツCCの解凍を開始させる（ステップS61）。

【0067】本発明方法は以上のような原理に基づいているが、以下に実際の実施の形態について説明する。

【0068】図11は本発明方法の第1の実施の形態を説明するための模式図である。なお、以下に説明するいずれの実施の形態においても、ユーザ側装置1とは本発明方法により有料または無料で配布される電子情報、即ちコンテンツを利用するユーザが使用するコンピュータシステムであり、またサーバ側装置2とはコンテンツCを有料または無料で配布する業者が自身で、または他の業者に委託して運営する管理側装置であり、更にユーザ側装置1とサーバ側装置2とはたとえば一般の公衆電話回線等の通信回線3で接続されており、いわゆるコンピュータ通信が可能である。

【0069】また、以下の各実施の形態においては、コンテンツC自体は自己解凍型のソフトウェアとして圧縮されたデジタルデータCCの状態でCD-ROM CDに記録されてユーザの手元に予め無料で配布されており、このCD-ROM CDには更に圧縮されたデジタルデータCCを自己解凍するための解凍プログラムUPと、この解凍プログラムUPを起動させるための処理を実行するユーザ側装置1用の実行プログラムEP1とが記録されている。また、ユーザ側装置1において実際に動作するのは実行プログラムEP1であり、サーバ側装置2において実際に動作するのは実行プログラムEP2である。

【0070】図11において、ユーザ側装置1では、まずユーザが自身のユーザID UIDを入力すると、それを実行プログラムEP1が通信回線3を介してサーバ側装置2へ送信させる。また同時に、ユーザは共有秘密情報としてのパスワードPWuをユーザ側装置1に入力する。このパスワードPWuが入力されると、実行プログラムEP1は乱数R1を発生し、この乱数R1とユーザID UIDとをパスワードPWuをパラメータとして暗号化部31に暗号化させて暗号化データE(R1//UID, PWu)を生成させ、申込番号としてユーザに提示する。

【0071】このようにして実行プログラムEP1が提示した申込番号E(R1//UID, PWu)をユーザが再度ユーザ側装置1に入力することにより、実行プログラムEP1はそれを通信回線3を介してサーバ側装置2へ送信させる。

【0072】サーバ側装置2では、ユーザ側装置1からユーザID UID及び申込番号E(R1//UID, PWu)を通信回線3を介して受信すると、実行プログラムEP2はパスワード検索部41にID/パスワードデータベース42に予め登録されて蓄積されている複数のユーザのユーザID UIDを検索させて登録済みのパスワードの中から対応するパスワードPWuを取り出させる。そして、実行プログラムEP2は、受信した申込番号E(R1//UID, PWu)をID/パスワードデータベース42から取り出した登録済みのパスワードPWcで復号化部43に復号化させ、乱数R1とユーザID UIDを得る。

【0073】次にサーバ側装置2では、実行プログラムEP2が、復号化部43により得られたユーザID UIDを先にユーザ側装置1から受信したユーザID UIDと比較部45に比較させる。この比較結果が一致した場合には、実行プログラムEP2は新たに乱数R2を生成し、復号化部43で復号した乱数R1と新たに生成した乱数R2とを合わせたデータを暗号化部44にID/パスワードデータベース42から読み出した登録済みのパスワードPWcで暗号化させてキーE(R2//R1, PWc)を生成させ、通信回線3を介してユーザ側装置1へ送信させる。なお、暗号化部44でこのキーE(R2//R1, PWc)を生成する時点で、課金処理が必要であれば実行する。

【0074】このキーE(R2//R1, PWc)を受信したユーザ側装置1では、実行プログラムEP1が、キーE(R2//R1, PWc)を先にユーザ自身が入力したパスワードPWuで復号化部32に逆変換させることにより、乱数R1を得る。実行プログラムEP1は、この復号化部32で得られた乱数R1を先に自身が発生した乱数R1と比較部33に比較させ、一致していれば自己解凍プログラムUPを起動して圧縮されているコンテンツCCの解凍を開始させる。

【0075】このように、図11に示されている第1の実施の形態では、ユーザはユーザ側装置1に対してユーザID UIDとパスワードPWuとを入力する。ユーザが入力したユーザID UIDは平文でサーバ側装置2へ送信されると共に、乱数R1と共にパスワードPWuで暗号化されて申込番号としてサーバ側装置2へ送信される。

【0076】サーバ側装置2では、平文で受信したユーザID UIDからID/パスワードデータベース42に蓄積されているユーザの登録済みパスワードPWcを検索し、これで申込番号を復号化し、その結果得られるユーザID UIDとと平文で受信したユーザIDUIDとを比較することによりユーザの認証が行なわれる。

【0077】また、サーバ側装置2では申込番号を復号化して得られた乱数R1を再度暗号化してユーザ側装置1へキーとして送信し、ユーザ側装置1ではこのキーを復号化して得られる乱数R1と先に自身が発生してサーバ側装置2へ送信した乱数R1とを比較することによりサーバの認証が行なわれる。

【００７８】図12は本発明方法の第２の実施の形態を説明するための模式図である。ユーザ側装置１では、まずユーザが自身のユーザID UIDを入力すると、それを実行プログラムEP1 が通信回線３を介してサーバ側装置２へ送信させる。

【００７９】これに対して、サーバ側装置２では、実行プログラムEP2 が乱数 R1 を発生して通信回線３を介してユーザ側装置１へ送信させるが、その際にユーザID UIDに対応するパスワードで暗号化した上で送信させる。具体的には、サーバ側装置２では、実行プログラムEP2 が、ユーザ側装置１から受信したユーザID UIDに従ってパスワード検索部41に ID/パスワードデータベース42に予め登録されて蓄積されている複数のユーザのユーザIDを検索させて登録済みの共有秘密情報の中から対応するパスワードPWc を取り出させる。そして、実行プログラムEP2 は、乱数R1をデータベース42から取り出した登録済みのパスワードPWc で暗号化部441 に暗号化させてデータE(R1, PWc)を得る。実行プログラムEP2 はこの暗号化部441により得られたデータE(R1, PWc)を受付番号として通信回線３を介してサーバ側装置２へ送信させてユーザに提示する。

【００８０】ユーザは、このサーバ側装置２から提示された受付番号E(R1, PWc)とパスワードPWu とユーザID UIDとをユーザ側装置１に入力する。実行プログラムEP1 はユーザが入力したパスワードPWu により受付番号E(R1, PWc)を復号化部321 に復号化させて乱数R1を取り出す。次に実行プログラムEP1 は新たに乱数R2を生成し、これと復号化部321 で得られた乱数R1とを合わせてパスワードPWu で暗号化部31に暗号化させてデータE(R2//R1, PWu)を生成させ、これをユーザに申込番号として提示する。

【００８１】このようにして実行プログラムEP1 が提示した申込番号E(R2//R1, PWu)をユーザが再度ユーザ側装置１に入力することにより、実行プログラムEP1 はそれを通信回線３を介してサーバ側装置２へ送信させる。

【００８２】サーバ側装置２では、ユーザ側装置１から申込番号E(R2//R1, PWu)を通信回線３を介して受信すると、実行プログラムEP2 が、先に ID/パスワードデータベース42から取り出してあるパスワードPWc で申込番号E(R2//R1, PWu)を復号化部43に復号化させて乱数R1, R2 を得る。

【００８３】次にサーバ側装置２では、実行プログラムEP2 が、復号化部43が得た乱数R1を先にユーザ側装置１へ暗号化して送信した乱数R1と比較部45に比較させる。この比較結果が一致していれば、実行プログラムEP2 は新たに乱数R3を生成し、この乱数R3と先に復号化部43で得られた乱数R2とを合わせたデータを先にデータベース42から読み出した登録済みのパスワードPWc で暗号化部442 に暗号化させてキーE(R3//R2, PWc)を生成させ、通信回線３を介してユーザ側装置１へ送信させる。なお、

暗号化部442 でこのキーE(R3//R2, PWc)を生成する時点で、課金処理が必要であれば実行する。

【００８４】このキーE(R3//R2, PWc)を受信したユーザ側装置１では、実行プログラムEP1が先にユーザ自身が入力したパスワードPWu をキーE(R3//R2, PWc)で復号化部322 に復号化させることにより、乱数R2, R3を得る。実行プログラムEP1 は、この復号化部322 で得られた乱数R2を先に自身が発生した乱数R2と比較部33に比較させ、一致していれば自己解凍プログラムUPを起動して圧縮されているコンテンツCCの解凍を開始させる。

【００８５】このように、図12に示されている第２の実施の形態では、サーバ側装置２から乱数R1をユーザの登録済みのパスワードPWc で暗号化して受付番号としてユーザ側装置１へ送信し、ユーザ側装置１では受付番号をユーザが入力したパスワードPWu で復号化することにより得られる乱数R1を、新たに発生した乱数R2と共に再度ユーザが入力したパスワードPWu で暗号化して申込番号としてサーバ側装置２へ送信する。サーバ側装置２では申込番号をユーザの登録済みのパスワードPWcで復号化して得られる乱数R1を先に自身が発生して暗号化してユーザ側装置１へ送信した乱数R1と比較することによりユーザ認証が行なわれる。

【００８６】また、サーバ側装置２では申込番号を復号化して得られた乱数R2をユーザの登録済みのパスワードPWc で再度暗号化してキーとしてユーザ側装置１へ送信し、ユーザ側装置１ではこのキーをユーザが入力したパスワードPWu で復号化して得られた乱数R2と先にユーザ側装置１へ送信した乱数R2と比較することによりサーバ認証が行なわれる。

【００８７】なお第３の実施の形態として、上述の図12の模式図に示されている第２の実施の形態において、サーバ側装置２からユーザ側装置１へ乱数R1を暗号化して送信する際に平文で送信するようにしてもよい。

【００８８】図13は本発明方法の第４の実施の形態を説明するための模式図である。ユーザ側装置１では、まずユーザが自身のユーザID UIDを入力すると、それを実行プログラムEP1 が通信回線３を介してサーバ側装置２へ送信させる。

【００８９】これに対して、サーバ側装置２では、実行プログラムEP2 は、ユーザ側装置１から受信したユーザID UIDに従ってパスワード検索部41に ID/パスワードデータベース42に予め登録されて蓄積されている複数のユーザのユーザIDを検索して登録済みの共有秘密情報の中から対応するパスワードPWc を取り出させる。次に実行プログラムEP2 は、乱数R1を発生し、この乱数R1と、ユーザID UIDと、予め定められているサーバ側の公開鍵Kpとを合わせて ID/パスワードデータベース42から先に取り出した登録済みのパスワードPWc で暗号化部441 に暗号化させてデータDES(R1//UID//Kp, PWc) を生成させ、受付番号として通信回線３を介してユーザ側装置１へ送

信させる。ユーザ側装置1ではこの受付番号をユーザに提示する。

【0090】ユーザは、このサーバ側装置2から提示された受付番号DES(R1//UID//Kp, PWc) と、ユーザID UIDと、パスワードPWu とをユーザ側装置1に入力する。これにより、実行プログラムEP1 は受付番号DES(R1//UID//Kp, PWc) をパスワードPWuにより復号化部321 に復号化させてデータR1, UID を取り出す。そして、実行プログラムEP1 は復号化部321 で復号化されたUID と先にユーザが入力したユーザID UIDとを比較部331 に比較させる。この比較部331 での比較結果が一致すれば、実行プログラムEP1 は新たに乱数R2を生成し、この乱数R2とパスワードPWu とを合わせて先に復号化部321 で復号化された公開鍵Kpにより暗号化部31に暗号化させ、得られたデータRAS(R2//PWu, Kp)を申込番号としてユーザに提示する。

【0091】このようにして実行プログラムEP1 が提示した申込番号RAS(R2//PWu, Kp)をユーザが再度ユーザ側装置1に入力することにより、実行プログラムEP1 はそれを通信回線3を介してサーバ側装置2へ送信させる。

【0092】サーバ側装置2では、ユーザ側装置1から申込番号RAS(R2//PWu, Kp)を通信回線3を介して受信すると、実行プログラムEP2 が秘密鍵Ksにより復号化部43に復号化させて乱数R2とパスワードPWu とを得る。

【0093】次にサーバ側装置2では、実行プログラムEP2 が、復号化部43が取り出したパスワードPWu と先にパスワード検索部41が ID/パスワードデータベース42から取り出した登録済みのパスワードPWc とを比較部45に比較させる。この比較結果が一致した場合には、実行プログラムEP2 は新たに乱数R3を生成し、この乱数R3と先に復号化部43により得られた乱数R2とを合わせたデータをデータベース42から読み出した登録済みのパスワードPWc により暗号化部442 に暗号化させたデータE(R3//R2, PWc)を生成させる。このデータE(R3//R2, PWc)はキーとして、通信回線3を介してユーザ側装置1へ送信される。なお、暗号化部442 でこのキーE(R3//R2, PWc)を生成する時点で、課金処理が必要であれば実行する。

【0094】このキーE(R3//R2, PWc)を受信したユーザ側装置1では、実行プログラムEP1が比較部332 にキーE(R3//R2, PWc)を先にユーザが入力したパスワードPWu で復号化させることにより、乱数R2, R3を得る。実行プログラムEP1 は、この復号化部322 で得られた乱数R2を先に自身が発生した乱数R2と比較部332 に比較させ、一致していれば自己解凍プログラムUPを起動して圧縮されているコンテンツCCの解凍を開始させる。

【0095】このように、図13に示されている第4の実施の形態では、ユーザ側装置1からユーザID UIDを平文で送信し、これをサーバ側装置2ではユーザの登録済みパスワードPWu で暗号化してユーザ側装置1へ受付番号として送信する。ユーザ側装置1では受付番号をユーザ

が入力したパスワードPWu で復号化して得られたユーザID UIDとユーザ自身が入力したユーザID UIDとを比較することによりサーバ認証が行なわれる。

【0096】また、受付番号にはサーバ側装置2で発生された乱数R1と公開鍵Kpとが暗号化されて含まれているので、ユーザ側装置1では新たに乱数R2を発生してユーザが入力したパスワードPWu と共に公開鍵Kpで暗号化して申込番号としてサーバ側装置2へ送信する。サーバ側装置2では、申込番号を秘密鍵Ksで復号化して得られたパスワードPWu を登録済みのパスワードPWc と比較することによりユーザ認証が行なわれる。

【0097】更に、申込番号にはユーザ側装置1で発生された乱数R2が暗号化されて含まれているので、サーバ側装置2では新たに乱数R3を発生して登録済みパスワードPWc で暗号化してキーとしてユーザ側装置1へ送信する。ユーザ側装置1では、キーをユーザ自身が入力したパスワードPWu で復号化して得られた乱数R2と先に自身がサーバ側装置2へ送信したR2とを比較することにより再度のサーバ認証が行なわれる。

【0098】図14は本発明方法の第5の実施の形態を説明するための模式図である。ユーザ側装置1では、まずユーザが自身のユーザID UIDと、パスワードPWu と、コンテンツ固有情報（以下、コンテンツIDと言う)PIDとを入力すると、実行プログラムEP1 はパスワードPWu とコンテンツID PIDとに対して MD5部34に一方向性関数による処理を施させて暗号化鍵KYとイニシャルベクタIVとを生成させる。なお、コンテンツIDは、たとえばCD-ROM CD のラベル等に記載されている番号、またはCD-ROM CD そのものに記録されれている番号である。

【0099】次に、実行プログラムEP1 は MD5部34により生成された暗号化鍵KYとイニシャルベクタIVとにより暗号化部31にユーザID UIDとユーザ側装置1のハード/OS固有情報HID とを暗号化させ、データDES(HID//UID, IV, KY) を得る。このデータDES(HID//UID, IV, KY) は申込番号としてユーザに提示される。なお、ハード/OS固有情報HID は、ユーザ側装置1に固有のハードウェア、たとえばCPU, HDD等に付与されている固有の情報、またはユーザ側装置1にインストールされているOS (オペレーティングシステム) 固有の情報である。

【0100】ユーザがこの申込番号DES(HID//UID, IV, KY) をユーザ側装置1に入力すると、実行プログラムEP1 が通信回線3を介してサーバ側装置2へ送信させる。

【0101】サーバ側装置2では、ユーザ側装置1から申込番号DES(HID//UID, IV, KY) を通信回線3を介して受信すると、実行プログラムEP2 は、先に受信しているユーザID UIDに従ってパスワード検索部41に ID/パスワードデータベース42に予め登録されて蓄積されている複数のユーザのユーザIDを検索して登録済みの共有秘密情報の中から対応するパスワードPWc を取り出させる。そして実行プログラムEP2 は、この登録済みのパスワード

PWc と先にサーバ側装置2から受信しているコンテンツID PIDとに対して MD5部46に一方向性関数による処理を施させて暗号化鍵KYとイニシャルベクタIVとを生成させる。

【0102】次にサーバ側装置2では、実行プログラムEP2 が MD5部46で生成された暗号化鍵KYとイニシャルベクタIVとにより復号化部43にサーバ側装置2から先に受信している申込番号DES(HID//UID, IV, KY) を復号化させ、データHID//UIDを取り出させる。そして実行プログラムEP2 は、この復号化部43により取り出されたユーザID UIDが先にサーバ側装置2から受信しているユーザID UIDと比較部45に比較させる。なお、比較部45での比較の際に、課金処理が必要であれば実行する。

【0103】比較部45による比較結果が一致していれば、実行プログラムEP2 は新たに乱数R2を生成し、この乱数R2と先に MD5部46により得られている暗号化鍵KYとイニシャルベクタIVとで乱数R2とハード／OS固有情報HID とを暗号化部44に暗号化させてデータDES(R2//HID, IV, KY)を得る。この暗号化部44により得られたデータDES(R2//HID, IV, KY)はキーとして通信回線3を介してサーバ側装置2へ送信される。

【0104】このキーDES(R2//HID, IV, KY)を受信したユーザ側装置1では、実行プログラムEP1 がキーDES(R2//HID, IV, KY)を先に MD5部34が生成した暗号化鍵KYとイニシャルベクタIVとで復号化部32に復号化させることにより、ハード／OS固有情報HID を得る。実行プログラムEP1 は、この復号化部32で得られたハード／OS固有情報HID をユーザ側装置1のハード／OS固有情報HID と比較部33に比較させ、一致していれば自己解凍プログラムUPを起動して圧縮されているコンテンツCCの解凍を開始させる。

【0105】このように、図14に示されている第5の実施の形態では、ユーザ側装置1からユーザID UIDとコンテンツID PIDとを平文で送信し、これをサーバ側装置2ではユーザの登録済みパスワードPWc とコンテンツID PIDとを一方向性関数で処理して暗号化鍵KYをイニシャルベクタIVとを生成する。一方、ユーザ側装置1でもユーザ自身が入力したパスワードPWu とコンテンツID PIDとを一方向性関数で処理して暗号化鍵KYをイニシャルベクタIVとを生成し、ユーザID UIDとハード／OS固有情報HID とを暗号化して申込番号としてサーバ側装置2へ送信する。サーバ側装置2では申込番号を自身で生成した暗号化鍵KYをイニシャルベクタIVとで復号化して得られたユーザID UIDをユーザ側装置1から平文で送信されたユーザID UIDと比較することによりユーザ認証を行なう。

【0106】また、申込番号にはユーザ側装置1のハード／OS固有情報HID が暗号化されて含まれているので、サーバ側装置2ではこれを再度暗号化鍵KYをイニシャルベクタIVとで暗号化してユーザ側装置1へキーとして送信する。ユーザ側装置1では受信したキーを暗号化鍵KY

をイニシャルベクタIVとで復号化して得られたハード／OS固有情報HID と自身のハード／OS固有情報HID とを比較することによりサーバ認証が行なわれる。

【0107】なお、上述の各実施の形態においては、共有秘密情報としてユーザのパスワードを使用しているが、一方が公開鍵を使用して情報を暗号化し、他方が秘密鍵を使用してその暗号化された情報を復元する方法を採ることも可能である。

【0108】また、受付番号または申込番号をユーザに一旦提示した後にそれをユーザがユーザ側装置1に再入力した上でサーバ側装置2へ送信するようにしている実施の形態があるが、ユーザの介在なしに自動的にサーバ側装置2へ送信してもよいことは言うまでもない。

【0109】

【発明の効果】以上に詳述したように本発明によれば、サーバ側においてユーザのパスワードでコンテンツを暗号化してユーザ側へ送信することはないため、コンテンツを暗号化する必要がなく、サーバ側での負担が減少する。また、暗号化されたコンテンツを送信しないため、通信コストを削減することが可能になり、更に通信中にエラーが生じてユーザ側で完全なコンテンツを受信出来ないというような事態も生じない。

【0110】また、本発明によれば、サーバ側でコンテンツ毎の復号化キーを管理する必要がないため、この復号化キーが漏洩する虞もなくなる。従って、電子情報（コンテンツ）を有料で配布する場合にも、経済的な損失を被る虞が減少する。

【図面の簡単な説明】

【図1】本発明方法の実施に使用されるシステム構成の一例を示す模式図である。

【図2】本発明方法の第1の原理を説明するための模式図である。

【図3】本発明方法の第1の原理のユーザ側装置の動作手順を示すフローチャートである。

【図4】本発明方法の第1の原理のサーバ側装置の動作手順を示すフローチャートである。

【図5】本発明方法の第2の原理を説明するための模式図である。

【図6】本発明方法の第2の原理のユーザ側装置の動作手順を示すフローチャートである。

【図7】本発明方法の第2の原理のサーバ側装置の動作手順を示すフローチャートである。

【図8】本発明方法の第3の原理を説明するための模式図である。

【図9】本発明方法の第3の原理のユーザ側装置の動作手順を示すフローチャートである。

【図10】本発明方法の第3の原理のサーバ側装置の動作手順を示すフローチャートである。

【図11】本発明方法の第1の実施の形態を説明するための模式図である。

27

【図１２】本発明方法の第２及び第３の実施の形態を説明するための模式図である。

【図１３】本発明方法の第４の実施の形態を説明するための模式図である。

【図１４】本発明方法の第５の実施の形態を説明するための模式図である。

【図１５】従来技術の一例の説明図である。

【図１６】従来技術の他の例の説明図である。

【符号の説明】

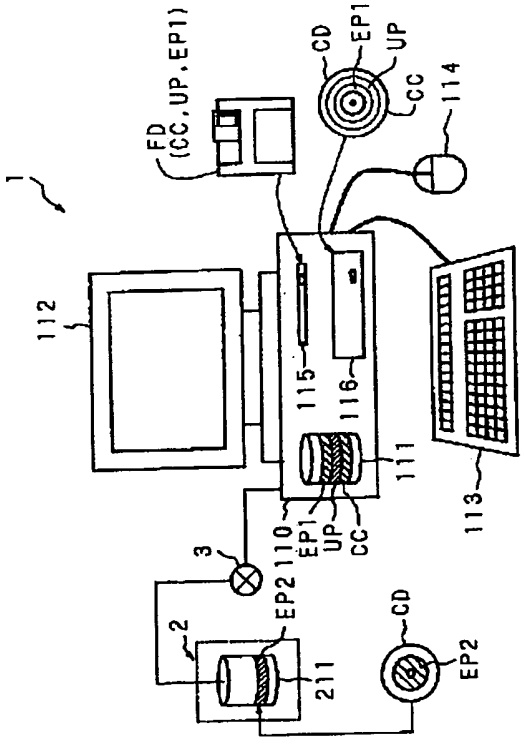
1　ユーザ側装置
2　サーバ側装置
3　通信回線
31　データ変換部（暗号化部）
32　データ逆変換部（データ逆変換部）
33　比較部
34　変換パラメータ生成部(MD5部)
41　共有秘密情報検索部（パスワード検索部）
42　データベース(ID/パスワードデータベース)
43　データ逆変換部（復号化部）
44　データ変換部（暗号化部）

28

45　比較部
46　変換パラメータ生成部(MD5部)
UID　ユーザID
Su　共有秘密情報（ユーザ側装置）
Ss　共有秘密情報（サーバ側装置）
R1, R2, R3　乱数
HID　ハード／OS固有情報
PID　コンテンツID
KY　変換パラメータ
PWu　パラメータ（ユーザ側装置）
PWc　パラメータ（サーバ側装置）
CD　CD-ROM
FD　フレキシブルディスク
111　ハードディスク（ユーザ側装置）
211　ハードディスク（サーバ側装置）
C　コンテンツ
CC　圧縮されたコンテンツ
UP　自己解凍プログラム
EP1　実行プログラム（ユーザ側装置）
EP2　実行プログラム（サーバ側装置）

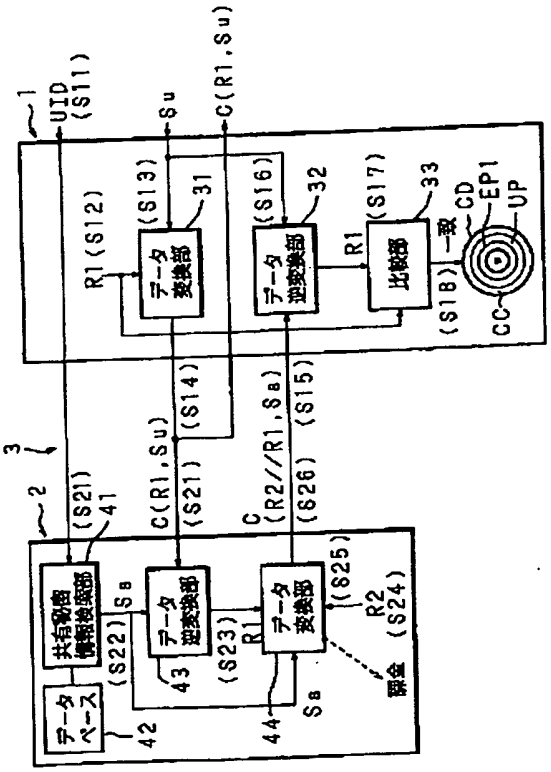
【図１】

本発明方法の実施に使用されるシステム構成の一例を示す模式図



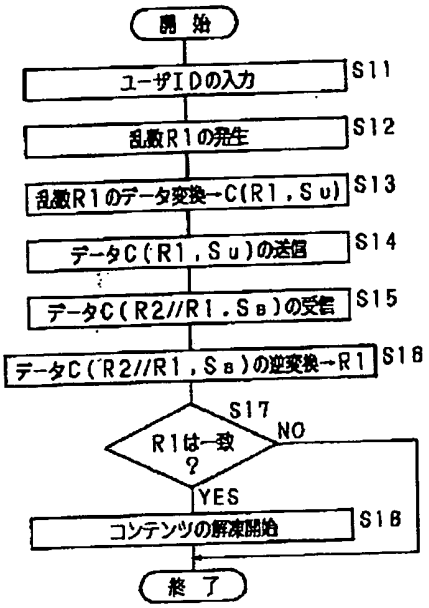
【図２】

本発明方法の第１の原理を説明するための模式図



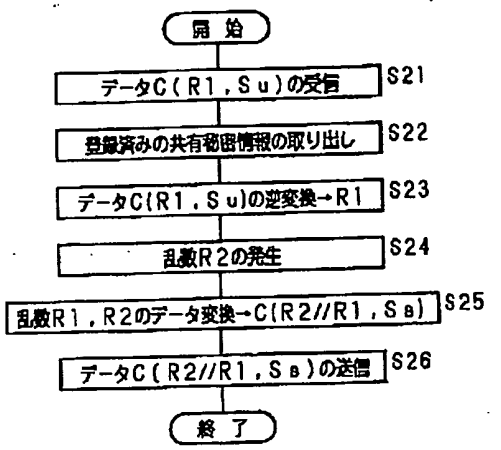
【図3】

本発明方法の第1の原理のユーザ側装置の動作手順を示すフローチャート



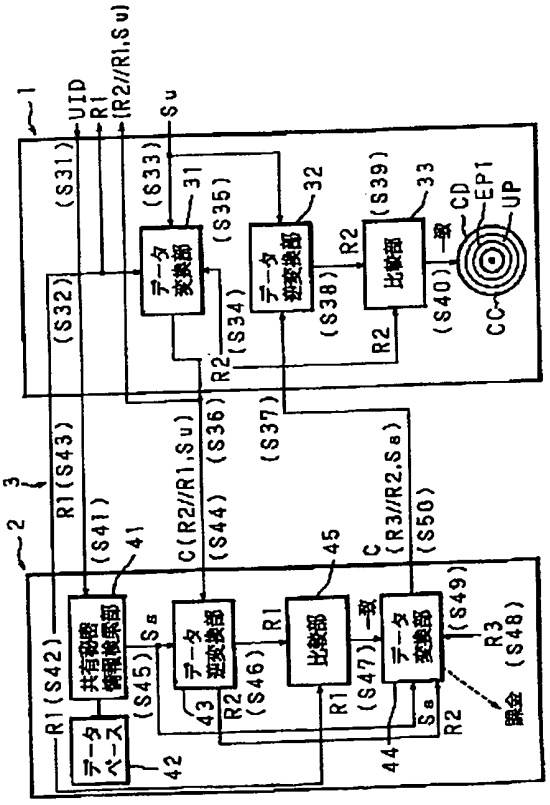
【図4】

本発明方法の第1の原理のサーバ側装置の動作手順を示すフローチャート



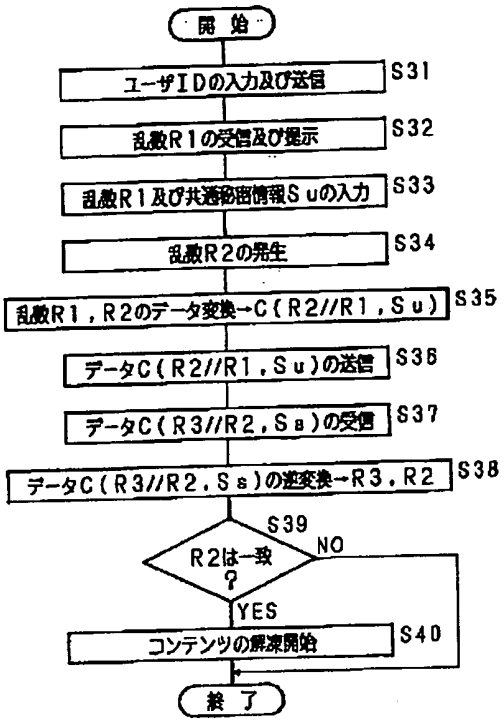
【図5】

本発明方法の第2の原理を説明するための模式図



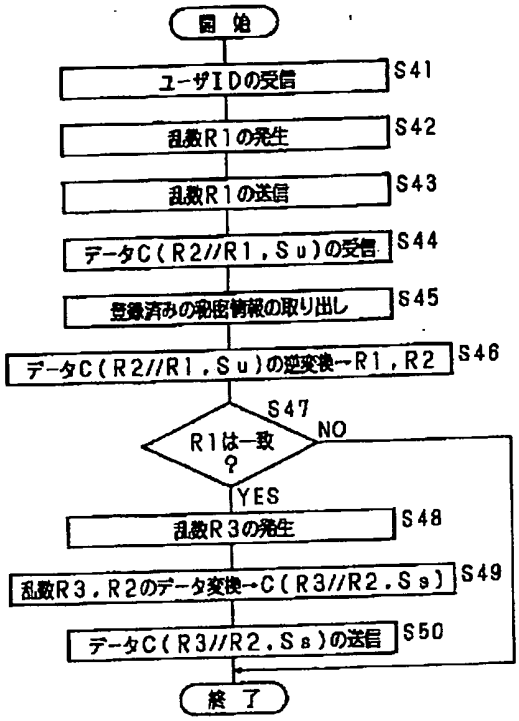
【図6】

本発明方法の第2の原理のユーザ側装置の動作手順を示すフローチャート



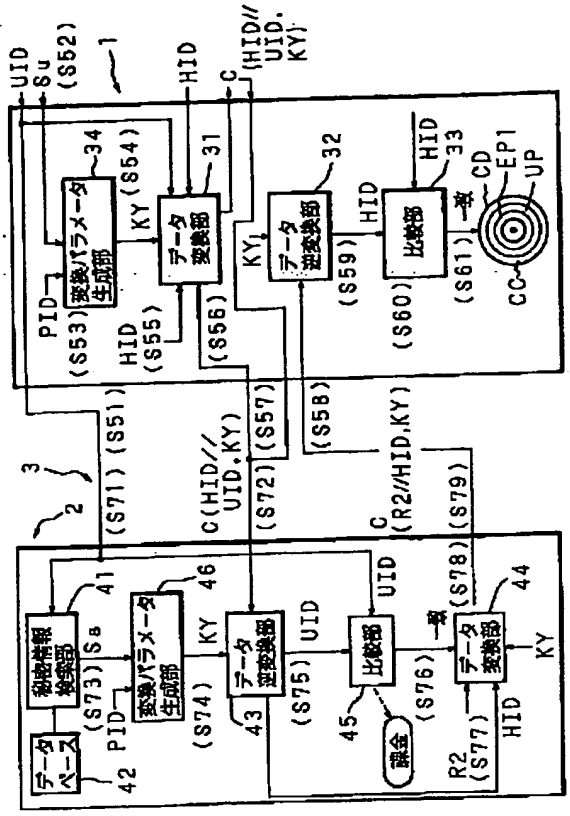
【図7】

本発明方法の第2の原理のサーバ側装置の動作手順を示すフローチャート



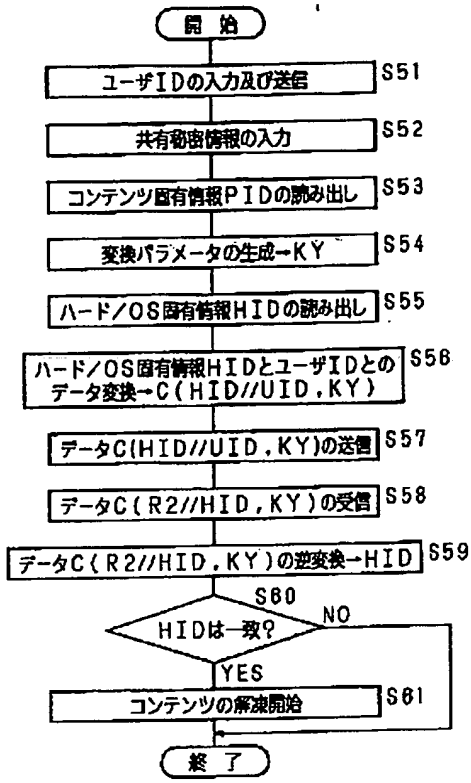
【図8】

本発明方法の第3の原理を説明するための模式図



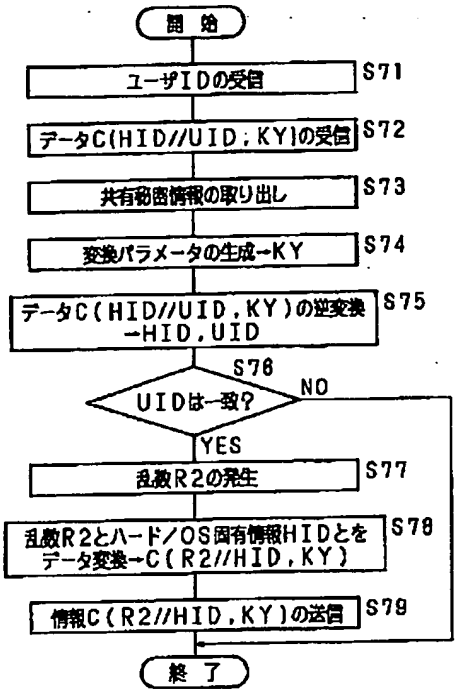
【図9】

本発明方法の第3の原理のユーザ側装置の動作手順を示すフローチャート



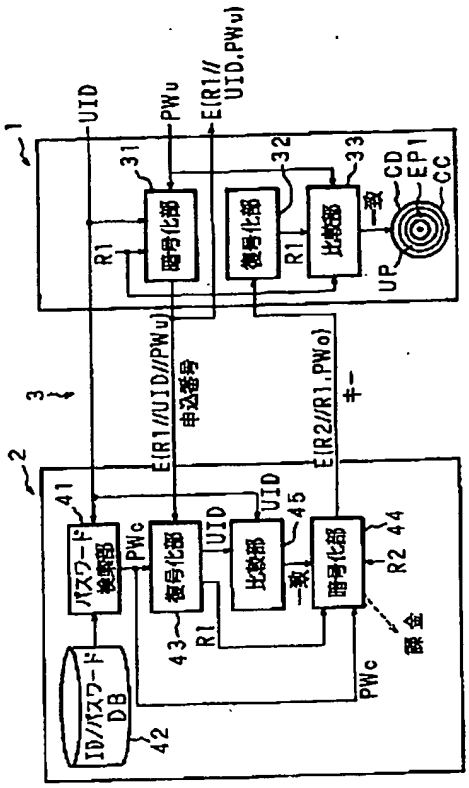
【図10】

本発明方法の第3の原理のサーバ側装置の動作手順を示すフローチャート



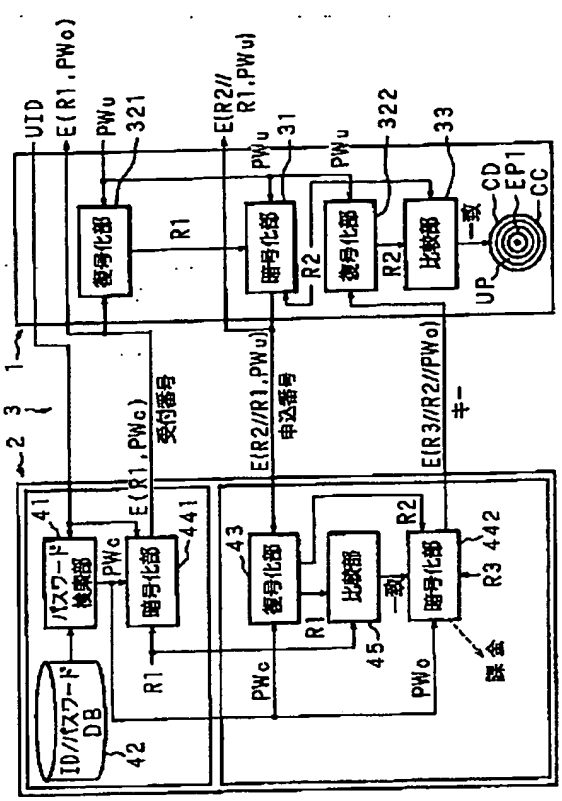
【図11】

本発明方法の第1の実施の形態を説明するための模式図



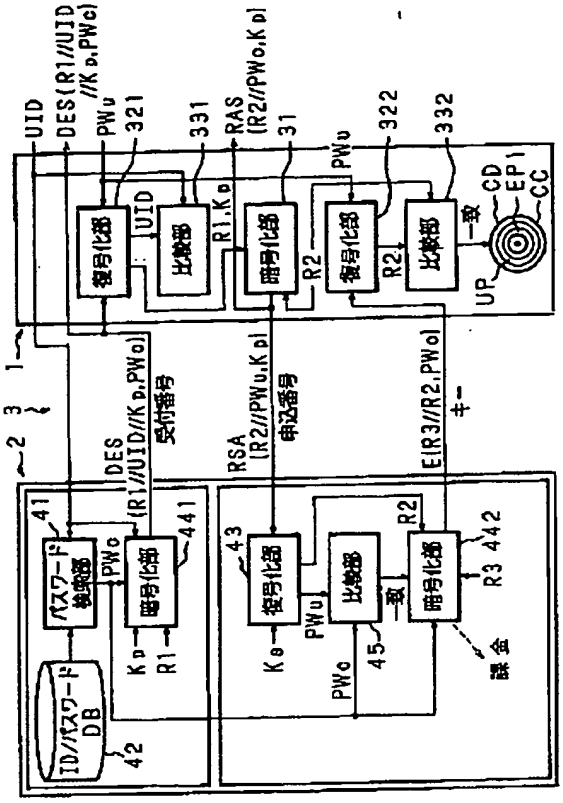
【図12】

本発明方法の第2及び第3の実施の形態を説明するための模式図



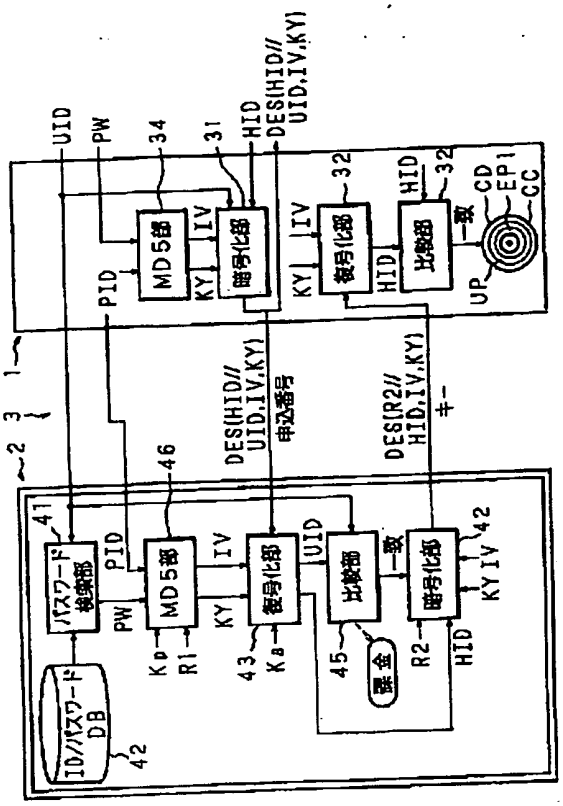
【図13】

本発明方法の第4の実施の形態を説明するための模式図



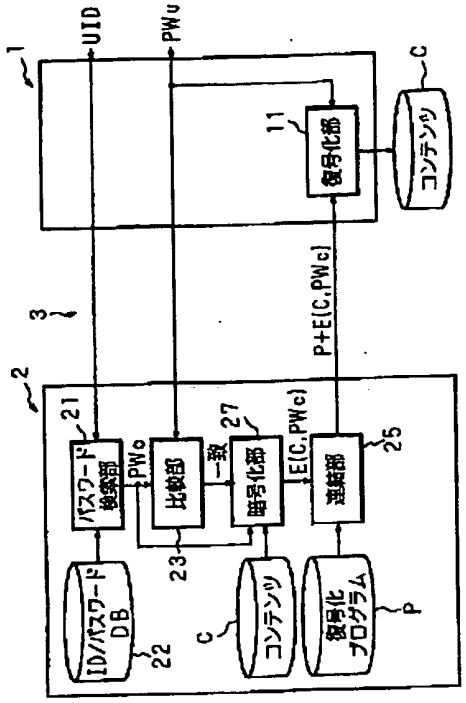
【図14】

本発明方法の第5の実施の形態を説明するための模式図



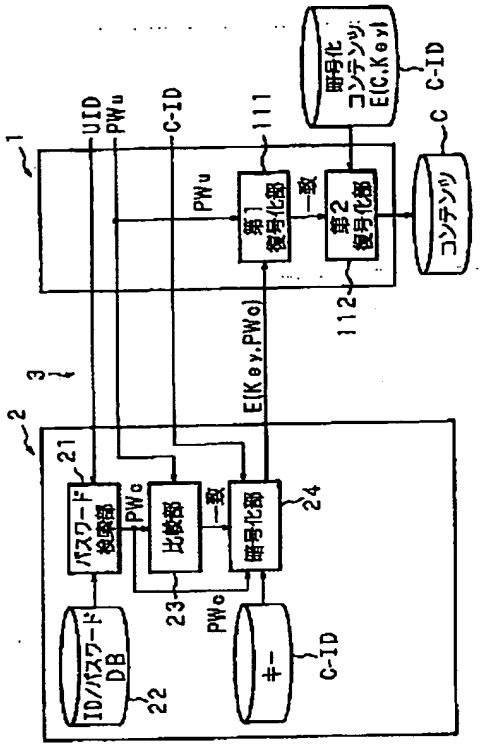
【図15】

従来技術の一例の説明図



【図16】

従来技術の他の例の説明図



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
G11B 20/10		G11B 20/10	H
H04L 9/32		H04L 9/00	675A

(72)発明者　平賀　正浩
東京都港区海岸3丁目9番15号　株式会社ジー・サーチ内

(72)発明者　伊藤　千秋
東京都港区海岸3丁目9番15号　株式会社ジー・サーチ内